Studentská Vědecká Konference 2010

BEZPEČNOST V AKTIVNÍCH SÍTÍCH

Vladimír Aubrecht[1]

1 ÚVOD

Aktivní sítě nabízejí programovatelnost směrovačů, díky čemuž je možné vytvářet inteligentní směrovací a cachovací algoritmy, výrazně zlepšit kvalitu audio/video služeb nebo se vyhnout například dlouhodobému procesu standardizace nových protokolů.

Přesto, že aktivní sítě mají spoustu svých pozitiv, existují samozřejmě i negativa, která do dnešních dnů brání většímu rozšíření aktivních sítí. Dvěmi zásadními negativy jsou bezpečnost a náročnost tohoto řešení.

V klasických sítích se spokojíme s relativně nízkým výkonem směrovačů, protože většinu času nám stačí pouze přijímat a přeposílat pakety podle jejich cílových adres. Naproti tomu v aktivních síti, kapsule, nástupce paketu, může být svázán s programovým kódem, který by měl směrovač vykonat. A zde tak stoupají nároky na procesor a paměť, případně přenosovou kapacitu sítě.

Kapsule může být svázána s libovolným programovaým kódem. Nevznikají tak omezení díky standardizaci jako např. u IP a zároveň lze síť rychle naučit nové funkcionalitě. S programovatelností směrovačů je však svázán i problém s bezpečností. Je třeba zajistit, aby uživatelský program nezahltil směrovač, popř. aby nějakým způsobem nemodifikoval nebo nečetl cizí data.

Problematikou bezpečnosti aktivních sítí se dále zabývá moje diplomová práce v rámci projektu Smart Active Node (SAN), viz http://www.san.zcu.cz/

2 BEZPEČNOST V AKTIVNÍCH SÍTÍCH

Jak už bylo řečeno, bezpečnost je u aktivních sítí jedním z hlavních problémů. Má diplomová práce nabízí řešení pro nejvážnější bezpečnostní problémy.

Pojďme si je blíže přiblížit. Prvním bezpečnostním problémem, na který narazíme je problém se spotřebou zdrojů. Zdrojem se rozumí paměť, čas procesoru a přenosová kapacita. Je nutné, aby existovala pravidla, na základě kterých jsme schopni přidělovat zdroje běžícímu programovému kódu. A to tak, aby uzel aktivní sítě nebyl zahlcen ať už neúmyslně, či útokem.

Aby jsme tyto pravidla mohli aplikovat, je nutné nejprve rozlišit, které aplikace jsou důvěryhodné a které ne, popř. jak moc jsou důvěryhodné. Tohoto je docíleno zavedením uživatelských účtů a rolí, kde pro každou roli je definován profil s limity pro povolenou spotřebu zdrojů a prioritami pro jednotlivé role.

Po zavedení limitů a priorit již není problém omezovat API SAN serveru, plánovat běh jednotlivých aktivních kódů, popř. omezovat jejich využití paměti nebo využití kapacity síťě.

[1] Vladimír Aubrecht, student navazujícího studijního programu Inženýrská informatika, obor Softwarové inženýrství, e-mail: aubrechv@students.zcu.cz

Všechny tyto bezpečnostní opatření jsou zastřešeny tzv. bezpečnostním monitorem, který obsahuje správu uživatelských účtů, rolí, profily s limity, priority rolí, atp. Jeho hlavním účelem je stát se centrem bezpečnosti SAN serveru.

Mimo zastřešení již zmíněného se bezpečnostní monitor stará o povolení či zamítnutí prakticky jakékoliv akce v SAN serveru. To zahrnuje i problém s kontrolou vykonávaného aktivního kódu.

Problém vykonávaného kódu si lze ukázat na příkladu. Na server se odešle kapsule, kde jedinný obsah aktivního kódu bude volání: System.exit(0); Protože SAN server běží celý jako jeden proces, je nutné se těmto voláním bránit, protože jinak by se SAN server ukončil. Sice řádně z pohledu hostujícího systému, ale jinak by šlo o nežádoucí akci z pohledu sítě. Proto je nutné tomu zabránit – bezpečnostní monitor má právo veta při pokusu kódu o provední např. volání System.exit(0).

Dalším problémem jsou D/DoS útoky. Abychom se s nimi dokázali vypořádat, je vhodné monitorovat chování okolních uzlů a budovat si statistiku důvěryhodnosti jednotlivých uzlů. Důvěryhodnost vytváříme dvěma způsoby - staticky a dynamicky. Statickou důvěryhodnost získáme na základě autentizace a autorizace konkrétního uzlu. Dynamickou důvěryhodnost získáme na základě získaných statistik (např. např. detekujeme podezřelé nárůsty zátěže sousedního uzlu, či abnormality v počtu a chování příchozích kapsulí z daného uzlu).

3 ZÁVĚR

Aktivní sítě nabízejí nové možnosti, kterým klasické sítě nemohou konkurovat. Díky stále rychlejšímu hardware a zde zmíněnými bezpečnostními opatřeními se aktivní sítě zbavují svých dvou největších problémů. Jejich budoucnost tak čím dál tím více záleží na přijetí veřejností. Dlužno poznamenat, že využívání programovatelnosti sítě doprovázejí síťové technologie už od prvních konceptů sdílení zátěže - Worms.

LITERATURA

Jan Syrovátka, 2009, *Code Interpreter for Smart Active Node*, ZČU KIV.

Petr Štěpánek, 2009, *Code Distribution in Active Networks*, ZČU KIV.

Rejda Michal, 2008, *Smart Active Node*, ZČU KIV.